Document Duration	**1(one) year 2024/25**
Department	**Risk Management Strategy**
Document Owner	**Chief Risk Officer**

Table of Contents

1. Introduction
2. Legislative Framework
3. Objectives of the Strategy
4. Definitions
5. Enterprise Risk Management Processes (ISO 31000)
6. Review of Risk Management Strategy
7. Recommendation and Approval

1. INTRODUCTION

The Risk Management Strategy is aimed at outlining a plan on how the municipality will go about implementing its risk management strategy. It further articulates a plan of action to improve the municipality risk profile. In simpler terms, this document illustrates how ongoing risk management will work in the Municipality.

2. LEGISLATIVE FRAMEWORK

2.1 MFMA, section 62 (1) (c) (i)

2.1.1 The Accounting Officer of a municipality must take all reasonable steps to ensure that the municipality has and maintains effective, efficient and transparent systems of financial and risk management and internal control.

2.2 Treasury Regulations 3.2.1.

2.2.1 The Accounting Officer must ensure that a risk assessment is conducted regularly to identify emerging risks of the department.

2.2.2 A risk management strategy, which must include a fraud prevention plan, must be used to direct internal audit effort and priority, and to determine the skills required of managers and staff to improve controls and to manage these risks.

2.2.3 The strategy must be clearly communicated to all officials to ensure that the risk management strategy is incorporated into the language and culture of the department.

3. OBJECTIVES OF THE STRATEGY

3.1.1. The objective of the risk management strategy is to establish a formal mechanism that will facilitate the timely identification and management of risk

and, hence, ensure the delivery of the strategic plan objectives. It also includes the following:

3.1.2 Raising awareness of principles and benefits involved in the risk management processes and to obtain staff commitment to the principle of risk control;

3.1.3 Facilitate compliance with best practice in corporate governance, ensuring that the appropriate disclosure statement can be issued; and

3.1.4 Ensure that risk management activities are fully integrated into the planning, monitoring and reporting processes and into the daily management of program activities.

4 DEFINITIONS

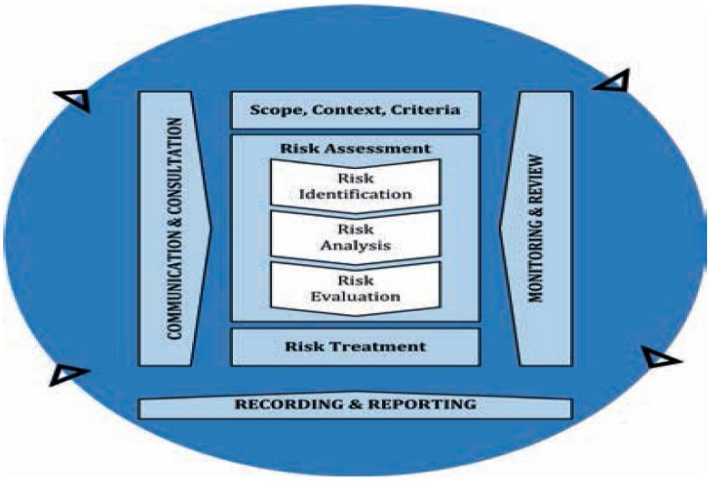
4.1 Risk - The possibility of an event occurring that will have a negative impact on the achievement of the department objectives.

4.2 Enterprise Risk Management - is the application of risk management throughout the department rather than only in selected business areas or disciplines.

ERM recognizes risks (including opportunities) as dynamic, often highly interdependent and ought not to be considered and managed in isolation.

4.3 Risk Management - a process to identify assesses, manage and control potential event in order to provide reasonable assurance regarding the achievement of the department's objectives.

5. ENTERPRISE RISK MANAGEMENT PROCESSES (ISO 31000)



5.1 Communication and Consultation

Communication and consultation with stakeholders, ensures clarity based on what their perceptions of the risk involved may be. Such perceptions are wide and varied, as individuals and programmes have different mandates, needs, assumptions, concepts and concerns.

Further, communication and consultation should be truthful, relevant, accurate and understandable, taking into account confidentiality and personal integrity.

External and internal risk communication and consultation strategy ensures that all the role-players who are responsible for the risk management process, as well as all the other stakeholders, understand the reasons and the actions required by risk-related decisions.

Consultative benefits may include:

- Describe the context properly.
- Ensure that stakeholders' interests are understood and taken into consideration.
- Ensure that risks are thoroughly and appropriately identified.
- Lead to cross-functional cohesion during the analysis of risks.
- Ensure that different viewpoints are considered while defining the risk criteria, and evaluating the risks.
- Help obtain backing from leadership and other stakeholders for the risk response plan.
- Support change management actions if the risk management process recommends any organisational changes.
- Lead to improvement of the external and internal risk communication and consultation strategy over time.

5.2 Establishment of Internal and External Context (Annexure A)

5.2.1 Internal Context

The internal context encompasses the following organisation-related aspects, amongst others:

- The objectives of the organisation, and the strategies and policies to comply to or achieve these.
- Organisational structure and governance.
- Leadership and senior management's roles and accountabilities.
- Resource and knowledge capabilities (i.e. capital, time, people, processes, systems and technology).
- The organisation's relationship with internal stakeholders, its perception of these stakeholders and the value it attaches to them.
- The organisational culture.
- Formal and informal systems for the acquisition, dissemination and retrieval of information.
- Decision-making processes and strategies.
- Adopted standards, guidelines and models.
- The structure and scope of contractual relationships.
- Environmental issues (i.e. internal physical environment, including space, ergonomics, and office layout).

5.2.2 External Context

It is crucial for management to understand external context, as it influences the Department and the forces exerted upon it by its particular industries, society and setting. All of this should be taken into account, along with the external stakeholders' expectations and concerns when considering risks.

The external context includes the following, amongst others:

- The sociocultural, natural, political, legal and regulatory, financial and economic, technological and market environments – on an international, national, regional and local scale.
- Consideration of Internal and External Stakeholder Analysis **(Annexure B)**

5.3 Risk and Opportunity Assessment

5.3.1 Identifying the risks and opportunity – Identification starts with understanding the Department's objectives. The purpose of completing an exercise is to identify, discuss and document risks and opportunities facing the Department.

5.3.1.1 Risk and Opportunity can be identified at three levels:

(a) Strategic: Used to guide the organization over a time period exceeding one year. This identification is usually performed by senior management.

(b) Operational: Used on day to day activities or line functions. This identification is usually performed at the supervisory level or by individual or work teams tasked with a particular assignment.

(c) Project: Used to develop and manage the current period activities. The process manager is usually responsible for monitoring the project risk.

5.3.1.2 The basic approach to identify risks is through Risk Management Workshop

5.3.1.3 Risk Categories **(Annexure C)**

5.3.2 Risk and Opportunity Analysis

Risks and Opportunities are assessed on the basis of the likelihood and the impact of its occurrence (Impact x Likelihood).

(a) Impact the severity should that risk occur and/ or advantages should opportunity be realised **(Annexure D)**

(b) Likelihood The probability of the risk and opportunity occurring **(Annexure E)**

Table 1: Risk and Opportunity assessment matrix

Extremely high	
High	
Moderate	
Low	

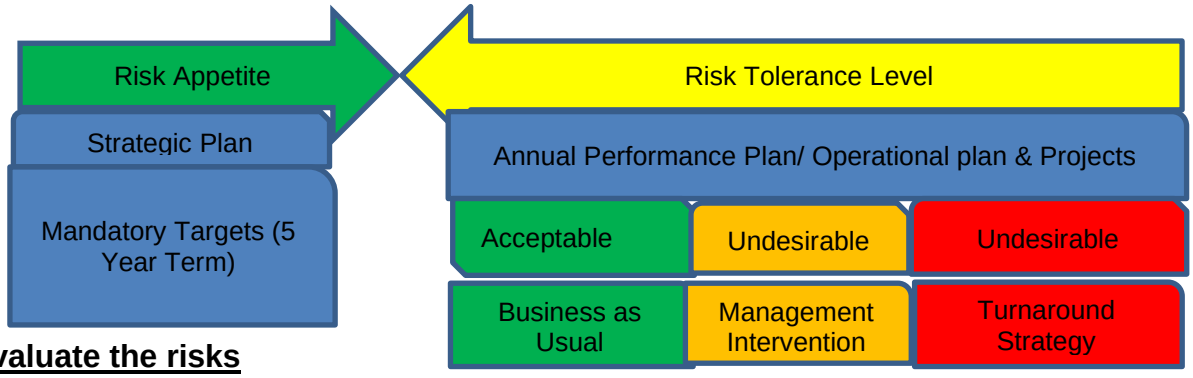
LIKELIHOOD											
	Almost certain	5	10	15	20	25	25	20	15	10	5
	Likely	4	8	12	16	20	20	16	12	8	4
	Moderate	3	6	9	12	15	15	12	9	6	3
	Unlikely	2	4	6	8	10	10	8	6	4	2
	Rare	1	2	3	4	5	5	4	3	2	1
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**	**High**	**Major**	**Moderate**	**Minor**	**Insignificant**
		IMPACT (Risk)					**IMPACT (Opportunities)**				

Risk rating determine the level of risk as:

(a) Risk Appetite - The amount of residual risk that the Institution is willing to accept.

(b) Risk Tolerance - The amount of risk the Institution is capable of bearing (as opposed to the amount of risk it is willing to bear)

The Department's Risk Appetite is to have low risk at (4) and the Risk Tolerance level at (8)



5.3.3 <u>Evaluate the risks</u>

This is the final step in the risk assessment process to evaluate the risk. This involves comparing the risk against pre-determined criteria, thus specifying the significance of the risk to the organisation's objectives.

<u>Risk evaluation involves interrogating risks at two levels</u>:

(a) Inherent risk

Involves considering the likelihood and impact of the risk in the absence of any management control intervention (provide perspective to management of the consequences of the risk to the department in its unmanaged state).

(b) Residual risk

The level of risk remaining after existing controls are implemented. The residual risk is a critical indicator of whether the existing controls are effective in reducing the risk to an acceptable level.

RISK LEVEL	RISK PRIORITISATION	ACTION AND LEVEL OF INVOLVEMENT REQUIRED
Low risk	Areas require no further review or attention	Accept, but monitor risk. Manage by routine procedures within the Programme
Moderate risk	Areas require management attention within next twelve months.	Management mitigation and an on-going monitoring required
High risk	Areas require management attention within next three months.	Inform Responsible Manager/ Senior Manager/ Head of Department
Extremely High risk	Areas require immediate management attention	Inform Responsible Manager/ Senior Manager/ Head of Department /Committees Immediate action required

5.3.4 Treatment of risks (Risk response)

The process of determining appropriate action the department will implement to mitigate the risks.

Identify risk response options

Strategy	Definition	Examples
Avoid	Anything you do to eliminate or prevent a risk from occurring	If the objectives are not met by Service Centers and Costs are higher than benefits, decision for closure may be enforced.
Reduce	Implement controls to reduce the likelihood and impact should the threat occur	Training of personnel, simulation and piloting of new processes, etc.
Transfer	Transfer the risks to a third party	Appointment of implementing agency/ entity to execute functions on behalf of the Department
Accept	Accept the risk without taking any measures after considering the tolerance level of the residual risk	When objectives are met and benefits are higher than the costs i.e. In-house training than outsourcing

Opportunities Response

Strategies	Definition	Examples
Realise (Exploit)	the realisation of an opportunity ensures that potential	Create a new process, product or service

	improvements to an organisational are delivered	
Enhance	action is taken to increase the likelihood, impact or both	Improve existing processes, products or services
Share	shared on a pain/gain share basis	Build or strengthen alliances, partnerships and relationships with both new and existing stakeholders
Accept	do absolutely nothing and accept the risk and its full impact should it occur incurring no costs at all	Reduce the use of various resources including financial or natural

Types of Controls activities

Control Types	Description
Preventative	Designed to discourage errors or irregularities from occurring e.g. adequate physical security of assets to prevent losses such as theft or damage,
Detective	Designed to find errors or irregularities after they have occurred e.g. performance of reconciliation procedures to identify errors,
Corrective measure	Operate together with detective controls in order correct identified errors or irregularities.

5.4 Monitoring and Review

Performance can be measured by evaluating the progress made by implementing the organisation's chosen risk response plans. These progress results can be incorporated into the organisation's overall performance management, performance measurement and its external and internal reporting activities.

Monitoring and review work must include planning, examining and evaluating, recording, communicating results and following up.

Risk maturity model will be utilised to determine the level of compliance with relevant Risk Management legislations **(Annexure F)**

Management reviews the effectiveness of risk management processes in terms of Key Performance Indicators as recommended by Fraud and Risk Management Committee.

5.4.1 Emerging risks

Emerging risks can be regarded as new risks that may be an imminent threat. New risks identified by institutions must follow protocol:

a) New risks identified by institutions must be submitted to the risk management unit.

b) The Department Risk Register will be scrutinized to determine whether or not it has already been included:

- If it is already been included in Department Risk Register, the institution may immediately include it in its own register;
- If it is not included in the Department Risk Register, it must be submitted to the Department Risk Management Committee for discussion; and
- If it is approved by the Risk Management Committee, the Department's Risk Register must be updated. This is to ensure

that the Department Risk Register reflects all the risks in the Department.

5.5 Recording and Reporting

The results of monitoring and reviewing risk should be recorded and reported (externally and internally) in an appropriate manner.

All activities of risk management undertaken should be traceable and noted, so that these records can serve as a foundation for improvement in methods and tools, as well as in the overall process **(Annexure G)**.

6. POLICY REVIEW

The custodian of this Policy is the Municipal Risk Management unit. The policy will be reviewed annually and submitted for approval to the council.

7. RECOMMENDATION AND APPROVAL

As approved/ adopted by means of council resolution **no: 1.68** in an ordinary/special Council, held at **Kroonstad** on the **07 November 2024.**

Annexure A: Risk categories

As the risk environment is so varied and complex it is useful to group potential events into risk categories. By aggregating events horizontally across an institution and vertically within operational units, allows the development of an understanding of the interrelationship between events to gain enhanced information as a basis for risk assessment.

The main categories to group individual risk exposures are provided below. **When using this template the institution should replace the Risk categories in this worksheet with the Risk categories approved by the institution:**

Risk type	Risk category	Description
Internal	Human Resources	Risks that relate to human resources of an institution. These risks can have an effect on an institution's human capital with regard to: • Recruitment; • Skills and competence; • Employee wellness; • Labour Relations; • Retention; and Tools of trade
	Knowledge and information management	Risks relating to an institution's management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management: • Availability of information; • Stability of the information; • Integrity of information data; • Relevance of the information; • Retention; and • Safeguarding.
	Litigation	Risks that the institution might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: • Claims by employees, the public, service providers and other third party • Failure by an institution to exercise certain rights that are to its advantage
	Loss \ theft of equipment	Risks that an institution might suffer losses due to either theft or loss of an asset of the institution.
	Service delivery	Every institution exists to provide value for its stakeholders. The risk will arise if the appropriate quality of service is not delivered to the citizens.
	Information Technology	The risks relating specifically to the institution's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: • Security concerns; • Technology availability (uptime); • Applicability of IT infrastructure; • Integration / interface of the systems; • Effectiveness of technology; and • Obsolescence of technology.

	Third party performance	Risks related to an institution's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Non - performance could include: • Outright failure to perform; • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.
	Health & Safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the institution.
	Disaster recovery / business continuity	Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: • Disaster management procedures; and • Contingency planning.
	Compliance \ Regulatory	Risks related to the compliance requirements that an institution has to meet. Aspects to consider in this regard are: • Failure to monitor or enforce compliance • Monitoring and enforcement mechanisms; • Consequences of non compliance; and • Fines and penalties paid.
	Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.
	Financial	Risks encompassing the entire scope of general financial management. Potential factors to consider include: • Cash flow adequacy and management thereof; • Financial losses; • Wasteful expenditure; • Budget allocations; • Financial statement integrity; • Revenue collection; and • Increasing operational expenditure. • Availability of material; • Costs and means of acquiring \ procuring resources; and • The wastage of material resources
	Cultural	Risks relating to an institution's overall culture and control environment. The various factors related to organisational culture include: • Communication channels and the effectiveness; • Cultural integration; • Entrenchment of ethics and values; • Goal alignment; and • Management style.

	Reputation	Factors that could result in the tarnishing of an institution's reputation, public perception and image.
	Risk category	**Description**
External	Economic Environment	Risks related to the institution's economic environment. Factors to consider include: • Inflation; • Foreign exchange fluctuations; and • Interest rates.
	Political environment	Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible factors to consider include: • Political unrest; • Political interference; • Local, Provincial and National elections; and • Changes in office bearers.
	Social environment	Risks related to the institution's social environment. Possible factors to consider include: • Unemployment; and • Migration of workers.
	Environmental Factors	Risks relating to the institution's natural environment and its impact on normal operations. Consider factors such as: • Depletion of natural resources; • Environmental degradation; • Spillage; and • Pollution.

Annexure B: Impact the severity should that risk occur

Impact	Description
Major (4)	Significant impact on the achievement of strategic objectives and targets relating to organisational plan.
Moderate (3)	Disruption of normal operations with limited effect on the achievement of strategic objections or targets relating to organisational plan.
Minor (2)	No material impact on achievement of the organisation's strategy or objectives.
Insignificant (1)	Negligible impact.

Annexure C: Likelihood the probability of the risk should it occur

Likelihood	Description
Almost certain (5)	The risk is almost certain to occur more than once within the next 12 months.
Likely (4)	The risk is almost certain to occur once within the next 12 months.
Moderate (3)	The risk could occur at least once within 2 – 5 years.
Unlikely (2)	The risk occur at least once within a year.
Rare (1)	The risk is least to occur.

ANNEXURE D: DEPARTMENT'S MATURITY LEVEL

Maturity Levels		**Level 1 (Naïve)**	**Level 2 (Novice)**	**Level 3 (Normalised)**	**Level 4 (Natural)**
Department level criteria	*Risk Management Framework(1)*	No formal risk management framework or structure in place	Early stage risk management program *and* framework	Formalised risk management program, framework, and strategy updated on an annual basis	Risk management performance is measured on a regular basis as part of an on-going improvement cycle
	Risk Management understanding (2)	Little knowledge of risk management discipline	Aware of risk management, not clear on how it may benefit the Department	Understanding of risk management across some parts of the Department	Sound knowledge of risk management and its value to the Department
	Risk Management processes - Risk Owner/ Champions/ (3)	No formal Risk Management activities undertaken	Conduct some risk management activities (ad hoc)	Formal risk management programme in place	Risk management embedded in the Department and decision making
	Alignment of strategies (4)	Risk Management not incorporated into Department's planning and strategic thinking	Aware of needs to conduct formalised risk management not clear on broader Department's benefits	Risk Management incorporated into Department's planning and strategic thinking	On-going scanning of the external and internal environment to ensure that the risk management strategy is relevant and effective at all times
	Coordination (5)	No coordination and/or communication between assurance providers	Ad hoc, limited coordination and/or communication between risk and control functions	Combined assurance and layers of defence effectively applied to optimise risk management in the Department	Continuous monitoring the implementation and effectiveness of Combined assurance
	Reporting (6)	Risk management reports, content, and cycles of reporting standardised	Limited reporting on risk management, and where done, mostly compliance driven	Ad hoc reporting on risk management, mostly done by divisions with a high risk focus	Effective risk management reports done as per programme, and integrated with other related reporting requirements of the Department